V and R *Cybersecurity* (2019) 2:4
https://doi.org/10.1186/s42400-019-0021-3

通读了；有新意 （怎么把markov和自私结合起来）//
本paper认为energy是 node变成自私节点的原因；采用markov链建模, 试图预测节点的状态
//paper本身写的不清楚； 状态转移图也疑似不正确；

*《能耗&内存逐渐加深 自私逐渐加深//新假设或者是个idea》

Cybersecurity

RESEARCH

Open Access

Semi Markov process inspired selfish aware co-operative scheme for wireless sensor networks (SMPISCS)

Kanchana Devi V* and Ganesan R

Abstract

In Wireless Sensor Network (WSN), energy and packet forwarding tendencies of sensor nodes plays a potential role in ensuring a maximum degree of co-operation under data delivery. This quantified level of co-operation signifies the performance of the network in terms of increased throughput, packet delivery rate and decreased delay depending on the data being aggregated and level of control overhead. The performance of a sensor network is highly inclined by the selfish behaving nature of sensor nodes that gets revealed when the residual energy ranges below a bearable level of activeness in packet forwarding. The selfish sensor node needs to be identified in future through reliable forecasting mechanism for improving the lifetime and packet delivery rate. Semi Markov Process Inspired Selfish aware Co-operative Scheme (SMPISCS) is propounded for making an attempt to mitigate selfish nodes for prolonging the lifetime of the network and balancing energy consumptions of the network. SMPISCS model provides a kind of sensor node's behavior for quantifying and future forecasting the probability with which the node could turn into selfish. Simulation experiments are carried out through Network Simulator 2 and the performance are analyzed based on varying the number of selfish sensor nodes, number of sensor nodes and range of detection threshold.

Keywords: Information security, Routing overhead, Selfish sensor nodes, Semi Markov process, Wireless sensor networks

Introduction

Wireless Sensor Networks (WSNs) comprise of a large number of low cost tiny sensors distributed in a specific region for facilitating the activity of data process through sensing capability (Chen et al. 2013a). The multi-hop, decentralized and self-organizing nature of sensor nodes make it suitable for gathering the essential environmental data such that it could be effectively employed in various range of applications such as agriculture, industry and military (Guo et al. 2013). The co-operation between the sensor nodes is essential as they are devoid of a fixed infrastructure and a centralized entity of control (Arun Korath and Vineeth 2011). The sensor nodes need to deliver its co-operation for the other interacting sensor nodes by ignoring its benefits for improving the lifetime of the network (Qiu et al. 2010). The limited computational capability, energy and storage potential of sensor nodes induces selfish activity of sensor nodes. In practical situations, it is even more complex when the sensor nodes deployed for different objectives react with selfish intent (Duan et al. 2014a). This selfish action of sensor nodes paralyses the normal activity delivered by the sensor nodes for ensuring effective packet forwarding process. The potential challenge of sensor network lies in the formulation of efficient forecasting technique that motivates the selfish sensor nodes to enforce normal operation in the network (Zhang et al. 2010).

* Correspondence: kanchanadevi@vit.ac.in
School of Computing Science and Engineering, VIT University Chennai Campus, Chennai, TamilNadu, India

Generally, reputation and incentive mechanism are considered to be the best option for enforcing better co-operation among the sensor nodes of the networks. The reputation mechanism explores the degree of collaboration of sensor nodes based on its past behavior rather than its present co-operation strategy opted (Reindl et al. 2010). They investigate the issue of misbehavior through the trust factors that are evaluated based on the parameters like packet forwarding potential and energy. Similarly, the incentive mechanisms target on rewarding a sensor node for its collaborative behavior or punish them for their malicious intent. Most of the proposed selfish node prevention schemes of the literature fail to predict the selfish intent of sensor nodes based on the present interactive index computed through direct or indirect trust value (Eswari and Vanitha 2013). Semi-Markov chain inspired forecasting approach is the phenomenal among the existing forecasting scheme for preventing selfish activity of sensor nodes under routing (George and Kumar 2013).

In this paper, SMPISCS based on Semi-Markov chain is proposed in this paper for preventing selfish sensor nodes from routing so as to improvise the sensor network lifetime and enforce maximum possibility of collaboration under data dissemination. The core objective of this proposed SMPISCS focuses on estimating the probability of each state that a sensor node could get transited during its process of routing. This objective focuses on the development of a Semi-Markov inspired accurate forecasting scheme that aids in better prediction for reactive decision making process related to the selfish intent of sensor nodes. The probe diagnostic routine used in SMPISCS is uniformly distributed and thus converge the Semi-Markov prediction process into Semi-Markov chain by assuming the probe diagnostic time to be non-exponential. The comparative evaluation of SMPISCS is also performed through three dimensions that study the influence of increasing the total number of sensor nodes, selfish sensor nodes and co-operation factor under different detection limits.

The major contributions of this proposed SMPISCS approach are,

i) The proposed SMPISCS is potential in forecasting the selfish intention of the sensor nodes in prior to the routing process through Semi-Markov Process, such that packet drops or decrease in cooperation between sensor nodes is prevented.
ii) The proposed SMPISCS predicts the transition probability of sensor nodes that has the maximum feasibility of becoming a selfish intent node by investigating the possible states that a sensor node can enter into.
iii) The proposed SMPISCS is also capable of identifying the transition probability of each and every sensor node state at any given point of time.

The roadmap of the forthcoming sections is discussed as follows. Section 2 lists and details on the potential selfish sensor node prevention schemes propounded in the literature for improving network lifetime. The problem description, network model, communication model and description about the implementation of SMPISCS is elaborated in section 3. The simulation environment and inferences derived from the simulation results are clearly portrayed and investigated in Section 4 and Section 5 highlights the conclusions, potential contributions and possible enhancements that could be derived from implementation of SMPISCS.

Related work

In this section, the significant contributions of the literature proposed for preventing selfish nodes in sensor nodes are discussed with their merits and limitations for motivating the formulation of SMPISCS.

Initially, an attempt known as Incentive Detection Technique (IDT) (Chen et al. 2013b) was made for preventing the issue of selfish nodes which is the potential misbehavior in wireless sensor networks. IDT enforces co-operation between the sensor nodes of the network using two modules that relates to the punishment and detection for malicious intent of selfish nodes. The first module is responsible for dynamically alternating the behavior of sensor nodes depending on packet forwarding potential and the second module performs detection based on the difference between the elucidated mean re-transmission counts identified for a sensor node to the maximum re-transmission count estimated for the same. IDT enforces co-operation between the sensor nodes of the network using two modules that relates to the punishment and detection for malicious intent of selfish nodes. The first module is responsible for dynamically alternating the behavior of sensor nodes depending on packet forwarding potential and the second module performs detection based on the difference between the elucidated mean re-transmission counts identified for a sensor node to the maximum re-transmission count estimated for the same. IDT is confirmed to reduce the false detection rate and at the same time, enhances the detection rate and throughput. Window-based Scheme (WBS) was proposed by Tripathi et al. (Tripathi et al. 2013) for reducing the degree of overhead incurred by the underlying detection technique. WBS explores the detection of selfish sensors based on three dimensions that pertain to the intensity of misbehavior, the influence produced by each type of sensor misbehavior and the overhead incurred for processing the activity of detection. WBS is

not only a detection scheme but also aims at isolating this malicious intent from routing. Thus WBS is found to minimize the false positive rate to an appreciable threshold.

Further, an Evolutionary Game-based Incentive Mechanism (EGIM) was proposed by Chen et al. (Chen et al. 2011) for adjusting the fitness of the node's forwarding approach through the determination of co-operation factor. This fitness function aids in converging the malicious intent of sensor nodes into reliable normal entities of the network. EGIM confirmed its performance by improving the throughput, packet delivery and reducing the routing overhead and energy consumptions. EGIM suffers from the limitations of computation overhead as they need to compute and adjust the co-operation factor depending on the kind of maliciousness induced by the sensor nodes of the network. Reputation-based uneven Clustering Routing Protocol (RUCRP) (Zhang et al. 2016) was proposed for selfishness by considering energy assessment and reputation determination. Unequal kind of clustering is used in RUCRP for controlling and maintaining the objective of energy conservation. The determined reputation entity and energy are considered as the indexes for enforcing the act of collaboration. RUCRP provides between detection rate as it uses multi-level indexes for quantifying the action of sensor nodes, but they fail in addressing the issue that arises due to routing overhead.

Furthermore, a Co-operative Game–Based Routing Approach (CGBRA) is an incentive mechanism proposed for handling security and energy conservation through the principle of cooperative game theory (Li et al. 2012). This CGBRA used the concept of rewarding the normal and selfish nodes for packet forwarding and punish them when they fail for forwarding packets. The nodes are forced to establish collaboration for maximizing the payoff value in the player game strategy. CGBRA enhances the rate of throughput by prolonging the network lifetime. Then, a Game Theory-based Node Behavior Regulation Scheme (GT-NBRS) was proposed for preventing selfish nodes in wireless sensor nodes (Lin et al. 2015). This GT-NBRS utilized two stages for regulating the behavior of sensor nodes in the sensor networks. In the first stage, VA-based game theory model was incorporated for regulating the behavior of sensor nodes and in the second stage, a transmission approach was incorporated for ensuring reliable data dissemination to the destined sink within the expected timestamp. This GT-NBRS scheme was proved to meet the theoretical requirements under reduced energy cost by balancing the energy cost with a view to extend the lifetime of the network.

In addition, Trust Support-based Malicious Node Determination Scheme (TS-MNDS) was proposed mainly for detecting and also for preventing malicious selfish nodes in the sensor network (Prathap et al. 2016). In this TS-MNDS, the data dissemination between each sensor node and the sink is always facilitated with selection of parent node. This process of selecting the parent node is always initiated by adding the identity and trust value computed for each individual sensor nodes in order to perform encryption only when the bytes are actually appended by the forwarding node. This option of selection facilitated by this TS-MNDS aided in identifying the malicious selfish sensor nodes in the network by the estimated trust and identities. Once the parent node is selected, the child nodes in the network are responsible for monitoring the parent in order to evaluate their reliability determined through successive and failure data transactions. This TS-MNDS iterates this process of parent selection in the beginning of each round of implementation by partitioning the complete time incurred in data transmission into multiple rounds with equal time utility. This TS-MNDS was determined to improve the rate of detection with reduced energy cost for facilitating a superior increase in the lifetime of the network. Finally, a Trust-based Lightweight Selfish Node Detection Scheme (TLSNDS) was proposed for identifying the concealed characteristics of malicious sensor nodes in the network (Rikli and Alnasser 2016). This TLSNDS was inferred to be potential in handling the issues that emerge due to the influence of selfish and jamming attack. This TLSNDS utilized a single level of trust in which each and every sensor node is responsible for monitoring and collecting neighbor one hop information that aids in evaluating the trustworthiness of the sensor nodes under participation. In TLSNDS, the trust value of the sensor nodes under participation is achieved for classifying them into genuine and selfish nodes in the network. This TLSNDS was also formulated as an effective trust model that detects concealed characteristics of sensor nodes through the utilization of minimum power and memory. The results of the TLSNDS was confirmed to improve the rate of detecting malicious selfishly behaving sensor nodes with increased throughput, packet delivery rate and, reduced energy cost and routing overhead.

The research challenges that motivated the formulation of the proposed SMPISCS scheme are,

i) The selfish node detection approaches propounded sofar has been designed to mitigate the selfish sensor nodes have not focused on the effective Semi-Markov model for prediction.
ii) The majority of the selfish node detection approaches proposed for mitigating selfish sensor nodes have enabled only a maximum classification

rate of 94.62% during its discrimination process between selfish and cooperative sensor nodes.

iii) The traditional forecasting models that derived the benefits of the exponential smoothing average method are not highly potential in accurate prediction of selfish behavior of sensor nodes.

The aforementioned shortcomings elucidated from each of the contributed works of the literature induced the need for formulating a Semi-Markov Chain inspired forecasting SMPISCS model.

Problem description and system model for SMPISCS

The problem description, network model, communication model and detailed description of SMPISCS are detailed in the forthcoming sections.

Problem description

SMPISCS is the significant selfish behavior forecasting scheme proposed for sensor networks in order to ensure effective packet dissemination and co-operation degree for facilitating maximum network lifetime. SMPISCS make use of the characteristic features of Semi-Markov Chain for isolating selfish nodes from the network through the use of the probe diagnostic routine. The probe diagnostic routine is efficient enough in converging the Semi-Markov process of detection to a Semi-Markov Chain as the interval of detecting selfishness behavior is not necessarily exponentially distributed. The probe diagnostic routine is potential in transmitting the probe packets to all the interacting sensor nodes of the network with a threshold diagnostic time. This transmission of probe packets is responsible for estimating the probable transition probability of sensor nodes in the network at each and every instant of time. The number of probe packets and time of transmitting probe packets is uniformly distributed with a lower and upper limit of 0 and T respectively. This problem of selfishness identification considers an average diagnostic time under the uniform distribution for ensuring rapid detection of intentionally behaving selfish sensor nodes.

The notations that are utilized in this proposed SMPISCS are presented in Table 1.

Table 1 The notations with its descriptions used in the proposed SMPISCS

Notations	Description
N_s	Number Of Sensor Nodes In The Network
$T_S * T_S$	Terrain Area
d_s	Inter-communication distance between sensor nodes
d_{re}	Reachable inter-communication distance between sensor nodes
E_e	Energy consumed for sending data in the free path
E_{trans}	Energy consumed for transmission
E_{amp}	Energy consumed for sending data in the multi-fading path
E_{fuse}	Energy consumed for sending data under fused path
l	Length in Bits of data
(C, S)	Sensor node with cooperative state and has possibility of transiting into its selfish state
C_r	The threshold energy probability of sensor nodes
$1 - C_s$	The complementary threshold energy probability of sensor nodes
β	Failure time of the sensor node operating in normal mode
β_s	Time to failure of the selfish nodes
μ	Time to re-energize the failed node to turn into a reliable mode
$\pi_{C,\ S}$	Transition probability of a sensor node from cooperative state to its selfish state
π_{NC}	Transition probability of a sensor node from non cooperative state to its cooperative state
$\pi_{F,\ F}$	Transition probability of a sensor node from failure state that could not be rehabilitated
$\pi_{C,\ C}$	Transition probability of a sensor node to retain its cooperative state
$U_d(0, T)$	Uniformly distributed probe diagnostic time
ST_i	Sojourn time
$PT_{(i,j)}$	General probability representing the transition of sensor node from one state to another
(F, F)	Sensor node with failure state and has no possibility of transiting into its cooperative state
(C, F)	Sensor node from cooperative state to its failure state
S_i	Sojourn time state
T_{PR}	Threshold probe diagnostic time
(N, C)	Sensor node from cooperative state to its non cooperative state
(N, D)	Sensor node from defective state to its cooperative state

Network model for SMPISCS

In the network model of SMPISCS, 'N_s'refers to the sensor nodes which are assumed to be disseminated randomly on the terrain area of '$T_S * T_S$ 'and the characteristic features of the deployed nodes are listed as follows:

i) The sensor nodes of the network initially possess the same value of energy, trust and behavior.

ii) The energy possessed by the base station of the network is always infinite and the network comprises of only one base station.

iii) The sensor nodes of the topology gather knowledge related to the present location of the sensor nodes even under the absence of capabilities like GPS.

iv) The sensor nodes of the network are set to be static after their deployment and they incur a different degree of energy depending on the energy model identified based on transmission.

Communication model for SMPISCS

The communication model used in SMPISCS is similar to the communication model used in (Heinzelman et al. 2002). This communication model depends on 'd_s'is the intercommunication distance among the sensor nodes and also the broadcast distance among the sensor nodes. This 'd_s'is estimated based on two constraints viz., '$d_{re} \leq d_s$ 'and '$d_{re} > d_s$'which represents the free-space model of the system and multipath-fading model of the system respectively using $d_s = \sqrt{\frac{N_{e(fs)}}{N_{e(mp)}}}$. Further, the energy incurred by the sensor nodes for transmitting and receiving 'l' bits of data is computed using $E_{trans}(l) = l \times E_e + l \times E_{fuse} \times d_{re}^2$ (free space model), $E_{trans}(l) = l \times E_e + l \times E_{am} \times d_{re}^4$ (multi-path fading model) and $E_{receive}(l) = l \times E_e$. Where 'E_e ', 'E_{amp}' and 'E_{fuse} 'represents the amount of energy consumed for sending data in the free path, multi-fading path and fusion.

Description of semi Markov process inspired selfish aware co-operative scheme

In this section, initially the base of Semi Markov Process has been explained. This model is derived using the benefits of Markov-Renewal Process (MRP), it is quietly a different kind of two dimensional Markovian Sequence. The MRP used in the Semi Markov Process is defined through the renewal kernel called transition probabilities considered as initial distribution. The counting process related to the Semi-Markov Process that permits the estimation of process regularity. The regularity in the Semi-Markov Process is enforced through the counting process by incorporating a finite number of sequential jumps over a finite time period.

In wireless sensor networks, the degree of co-operation rendered by active sensor nodes is found to be phenomenally significant when compared to the selfish sensor nodes as they misbehave in the network for preserving its energy such that they remain survival even though they cannot facilitate enough co-operations. The failure rate of co-operating and selfish nodes are found to be entirely different and further, the impact produced by the co-operating and selfish nodes of the network is found to exhibit deviation. Initially, the sensor nodes of the network are operating in reliable mode, then the network is referred to be in the state (C, C). In this context, let 'β','β_s' and 'μ 'denotes the time to failure time of the sensor node operating in normal mode, time to failure of the selfish nodes and time to re-energize the failed node to turn into a reliable mode as highlighted in Fig. 1.

The transition of the network into the state (C, S) occurs when the energy possessed by the sensor nodes of the network reaches below the probability of 'C_s'. This induces the normally operating sensor nodes to behave in the selfish way in order to remain active in the network. Similarly, the network remains in the state (C, S) when some of the selfish nodes of the network are towards failure, but maximum of the sensors are in reliable mode with the defection probability of 'C_r'. In contrast, if the failures of the sensor nodes are not able to be estimated with detection probability '$1 - C_s$ 'then the networks enter in the state (N, C). Likewise, if the failure of the selfish sensor nodes are estimated with the same detection probability '$1 - C_s$ ', the network enters into the state 'ND'. The probability 'C_s 'and 'C_r 'depends on the computation of direct and indirect trust factor performed in (Chen et al. 2015). The system enters into the state (S, S) when the latent failure (i.e, the energy threshold is not sufficient enough to exhibit either selfish or reliable mode) takes place in the network when they are in the state (C, S), NC and ND respectively. Thus the steady balance equations derived from the state transition diagram of SMPISCS are.

$$\mu\pi_{CS} = \pi_{CC}(\beta + \beta_S). \tag{1}$$

$$\mu\pi_{NC} + \beta_S\pi_{NC} = \pi_{CC}\beta(1-C_S). \tag{2}$$

$$\beta\pi_{ND} = \pi_{C,C}\beta_S(1-C_r). \tag{3}$$

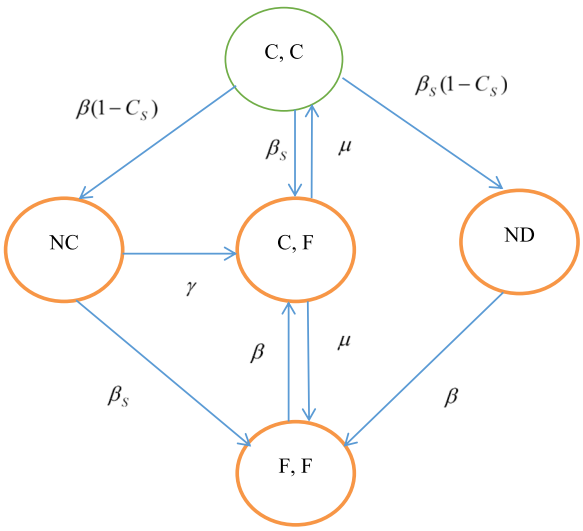

Fig. 1 State Transition Diagram of SMPISCS

$$\mu(\gamma+\beta_S)\pi_{FF}+\mu\pi_{FF}+\mu^2\pi_{FF} = \pi_{CC}(\beta+\beta_S)\beta+\pi_{CC}(\beta_S(1-C_r)) + \pi_{CC}(\beta+\beta_S)\beta_S. \quad (4)$$

The aforementioned steady state equations of SMPISCS are solved based on $\pi_{C,\,C}$and the steady state probabilities pertaining to the possible state behavior of sensor nodes of the network (Pal 2009) are obtained as.

$$\pi_{CS}=\frac{\pi_{CC}(\beta+\beta_S)}{\mu}. \quad (5)$$

$$\pi_{NC}=\frac{\pi_{CC}\beta(1-C_S)}{(\gamma+\beta_S)}. \quad (6)$$

$$\pi_{ND}=\frac{\pi_{CC}\beta_S(1-C_r)}{\beta}. \quad (7)$$

$$\pi_{FF}=\pi_{CC}\left(\frac{\beta(1-C_S)\beta_S}{\mu(\gamma+\beta_S)}+\frac{(\beta+\beta_S)\beta}{\mu^2}+\frac{\beta_S(1-C_r)}{\mu}\right). \quad (8)$$

Where

$$\pi_{CC}=\frac{1}{1+\frac{(\beta+\beta_S)}{\mu}\left(1+\frac{\beta}{\mu}\right)+\frac{\beta(1-C_S)}{(\gamma+\beta_S)}\left(1+\frac{\beta_S}{\mu}\right)+\beta_S(1-C_r)\left(\frac{1}{\beta}+\frac{1}{\mu}\right)}. \quad (9)$$

In this context, a probe routine is incorporated for identifying the selfish behavior in the network which repetitively run for 'T_{PR}'units. The sensor node (reliable or selfish) of the network possesses the failure and re-energize time which inspires exponential distribution, but the time interval of incorporating the run of probe routine for detection is not exponentially distributed. Thus SMPISCS fails to possess the characteristic properties of continuous Markov chain (Wereley and Walker 1988). But, SMPISCS is found to unveil the properties of Semi-Markov process because the change in state of the network form (N, D) to (C, S) is influenced by the sojourn time that depends on the amount of time duration, the network was under the state (N, D) rather than the past state. This Semi-Markov inspired SMPISCS technique uses the approximation time, which is exponentially distributed with mean probe time of '$\frac{T}{2}$'. Hence the steady balance equations derived using (5–8) is solved through approximations and the solutions are obtained using.

$$\pi_{CS}=\frac{\pi_{CC}(\beta+\beta_S)}{\mu}. \quad (10)$$

$$\pi_{NC}=\frac{\pi_{CC}\beta(1-C_S)}{(\gamma+\beta_S)}. \quad (11)$$

$$\pi_{ND}=\frac{\pi_{CC}\beta_S(1-C_r)}{\left(\beta+\frac{2}{T}\right)} \quad (12)$$

$$\pi_{FF}=\pi_{CC}\left(\frac{\beta(1-C_S)\beta_S}{\mu(\gamma+\beta_S)}+\frac{(\beta+\beta_S)}{\mu^2}+\frac{\beta_S(1-C_r)}{\mu\left(\beta+\frac{2}{T}\right)}\right). \quad (13)$$

Where

$$\pi_{CC}=\frac{1}{1+\frac{(\beta+\beta_S)}{\mu}\left(1+\frac{\beta}{\mu}\right)+\frac{\beta(1-C_S)}{(\gamma+\beta_S)}\left(1+\frac{\beta_S}{\mu}\right)+\frac{\beta_S(1-C_r)}{(\lambda T+2)}\left(1+\frac{\beta}{\mu}\right)}. \quad (14)$$

From the enhanced steady state balancing equation under approximation, the states' $\pi_{C,\,S}$'and 'π_{NC} 'are not influenced by probe diagnostic time with is uniformly distributed with '$U_d(0,T)$' The Semi-Markov Process(SMP) of SMPISCS converges to a Semi-Markov chain and hence a transition labeled '$U_d(0,T)$ 'is added into the transition diagram of SMPISCS. Fig. 2 portrays the transition diagram of SMPISCS with Semi-Markov chain. In this Semi-Markov chain, each of the transitions is assumed to occur in two stages. During the first stage, SMP is found to be in state' S_i'with the sojourn time described by 'ST_i'and in the second step, SMP utilizes the probability of '$PT_{(i,j)}$ 'that emphasizes the possibility of sensor nodes to move from one state to the other. SMP in SMPISCS is represented using sojourn time 'ST_i'and transition probability '$PT_{(i,j)}$ '. SMP of SMPISCS infers that, except the state 'ND', the distribution of the sojourn time for the remaining states is exponentially distributed.

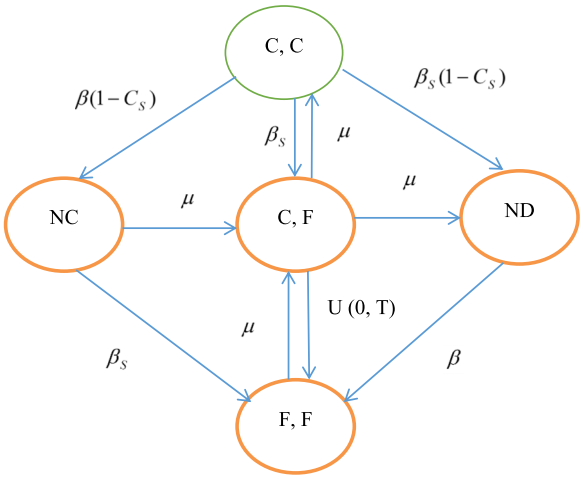

Fig. 2 Semi-Markov chain-based State Transition Diagram of SMPISCS

The sojourn time of 'ND' is determined by the minimum of exponential variable based 'β'and '$U_d(0,T)$ 'based random variable. Hence the sojourn time 'ST_i'of states in Semi-Markov chain-based SMPISCS are observed to be.

$$ST_{cc}(t) = 1-e^{-(\beta+\beta_S)t}. \tag{15}$$

$$ST_{CS}(t) = 1-e^{-(\gamma+\beta_S)t}. \tag{16}$$

$$ST_{CS}(t) = 1-\left(1-\frac{t}{T}\right)e^{-\beta t}, t \le T. \tag{17}$$

$$ST_{CS}(t) = 1, t \ge T. \tag{18}$$

$$ST_{FF}(t) = 1-e^{-\mu t}, t \ge T. \tag{19}$$

For determining the stochastic probability of transition from 'ND' to (C,S), let 'X' and 'Y' be considered as the random variables which represents the transition possibility 'β'and '$U_d(0,T)$ 'respectively. This probabilities need to be compared for analyzing whether the time required for the transition from 'NC' to '(C,S) is greater than the time required for the transition from 'ND' to '(C,S). If the transition time for the sensor node to transit from 'NC' to '(C,S) is greater than the time required for the sensor node to transit from 'ND' to '(C,S)'. is expressed using.

$$PT_{(X>Y)} = \frac{1}{\beta T}\left(1-e^{\beta T}\right). \tag{20}$$

The Discrete Time Markov Chain-based one-step transition probability matrix'M_{PT}' of SMPISCS is represented through.

	(C,C)	NC	(C,S)	ND	(F,F)
(C,C)	0	$\frac{\beta(1-C_S)}{(\beta+\beta_S)}$	$\frac{(\beta+\beta_S C_t)}{(\beta+\beta_S)}$	$\frac{\beta_S(1-C_t)}{(\beta+\beta_S)}$	0
NC	0	0	$\frac{\gamma}{(\gamma+\beta_S)}$	0	$\frac{\beta_S}{(\gamma+\beta_S)}$
(C,S)	$\frac{\mu}{\beta+\mu}$	0	0	0	$\frac{\beta}{\beta+\mu}$
ND	0	0	$\frac{1}{\beta T}(1-e^{-\beta T})$	0	$1-\frac{1}{\beta T}(1-e^{-\beta T})$
(F,F)	0	0	1	0	0

Then the five steady state probabilities of SMPISCS are computed using the vector V_{TP}= $[V_{(C,C)},V_{NC},V_{(C,S)}, V_{ND},V_{(F,F)}]$ and 'M_{PT} 'through equation$V_{TP} = V_{TP} * M_{PT}$. The sojourn time in each state 'i 'is derived as.

$$S_{(CC)} = \frac{1}{\beta+\beta_S}. \tag{21}$$

$$S_{NC} = \frac{1}{\gamma+\beta_S}. \tag{22}$$

$$S_{CS} = \frac{1}{\beta+\mu}. \tag{23}$$

$$S_{ND} = \frac{1}{\beta}-\frac{1}{T\beta^2}\left(1-e^{-\beta T}\right) \tag{24}$$

$$S_{(FF)} = \frac{1}{\mu}. \tag{25}$$

Finally, the state probabilities of SMPISCS are derived using '$\pi_i = \frac{V_{TP(i)*S_i}}{\sum_j V_{TP(i)*S_i}}$' in which$i, j \in \{(C,C), NC, (C,S), ND, (F,F)\}$. In this approach, the selfish behavior of sensor nodes is computed through the sum of state probabilities related to 'π_{NC}'and '$\pi_{(F,F)}$ 'respectively. Based on this summation value, the sensor nodes are identified as selfish when it reaches below the value of '0.3' as explained in (Ju et al. 2010).

Simulation results and discussions

In this section, the simulation environment, simulation parameters and performance metrics used for simulating the performance of SMPISCS is presented and the possible conclusions that are derived from the inferences are determined and elaborated as follows.

Simulation environment

The network area of simulation utilized for evaluating the performance of proposed SMPISCS and the benchmarked Co-operative Game–Based Routing Approach (CGBRA) Game Theory-based Node Behavior Regulation Scheme (GT-NBRS) Trust Support-based Malicious Node Determination Scheme (TS-MNDS) Trust-based Lightweight Selfish Node Detection Scheme (TLSNDS) is 200 × 200 meters with 200 as the maximum number of sensor nodes. The implementation of the proposed SMPISCS scheme and the benchmarked CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes are simulated by assigning the similar parameters in the simulation setup. The selfish sensor nodes are scattered uniformly in the topology. The number of selfish nodes is also varied dynamically during the process of simulation in order to study the influence of the proposed SMPISCS scheme towards the minimization of its impact in the network topology. The initial energy of the sensor nodes is assigned to 0.5 J and maximum number of rounds used for implementation are 800 rounds. The length of data and control packets are 4000 and 100 respectively, with 4200 bits of data packet size.

The additional parameters used for simulation are described in Table 2.

In the forthcoming section, the significance of SMPISCS in terms of its performance over CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes are discussed below.

Table 2 Simulation parameters for SMPISCS

Parameter description	Used value
Sensor nodes	200
Initial energy of sensor nodes	0.5J
Location of base station	(100,100)meters
Uniform speed distribution	(0,25)meters
Data packet size	4200 bits
Coverage area of the network	(0,0)-(200,200)
Maximum number of rounds	800
Length of control packets	100
Length of data packets	4000
Position of the sink	(0,0)

Results and discussions

The significance of SMPISCS used in the selfish sensor node detection is explored by investigating its performance in three dimensions. In the first dimension, SMPISCS is studied through packet delivery ratio, throughput, routing overhead and energy consumptions based on different numbers of sensor nodes of the network topology. In the second perspective, SMPISCS is explored using the same performance metrics similar to the first dimension of investigation under the influence of varying selfish sensor nodes of the network. Finally, the improvement in network lifetime of SMPISCS is analyzed under different thresholds of detection with a different co-operation degree of 0.3, 0.6 and 0.9 respectively.

Initially, packet delivery ratio, throughput, routing overhead and energy consumptions of the network is studied under the impact of dynamically varying sensor nodes. The packet delivery ratio and throughput of SMPISCS evaluated under different sensor nodes in the network field. The result emphasizes that SMPISCS is strong enough in facilitating maximum packet delivery rate and throughput than CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes. This result proves that the packet delivery rate of SMPISCS is improved to about 11%, 15%, 18% and 22% compared to CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes. The throughput is also found to improve by 13%, 15%, 17% and 20% due to the exploration possibility of transition behavior used in SMPISCS are presented in Figs. 3 and 4.

The routing overhead and energy consumption rate of SMPISCS explored under different sensor nodes in the network field. The result emphasizes that SMPISCS is suitable and capable of reducing the routing overhead and energy utilization rate over CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes by triggering a reliable probe-based exponentially varying diagnostic routine that aids in the rapid detection process. The result infers that the routing overhead of SMPISCS is minimized to the phenomenal level of 12%, 15%, 18% and 21% compared to CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes. Similarly, the energy consumptions of SMPISCS seem to get reduced by 7%, 10%, 13% and 16% higher than CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes unveils in Figs. 5 and 6.

In the second experimental investigation, packet delivery ratio, throughput, routing overhead and energy consumptions of the network is studied under the influence of different number of selfish sensor nodes. The packet delivery ratio and throughput of SMPISCS analyzed under different number of selfish sensor nodes in the network field. The result infers the potentiality of

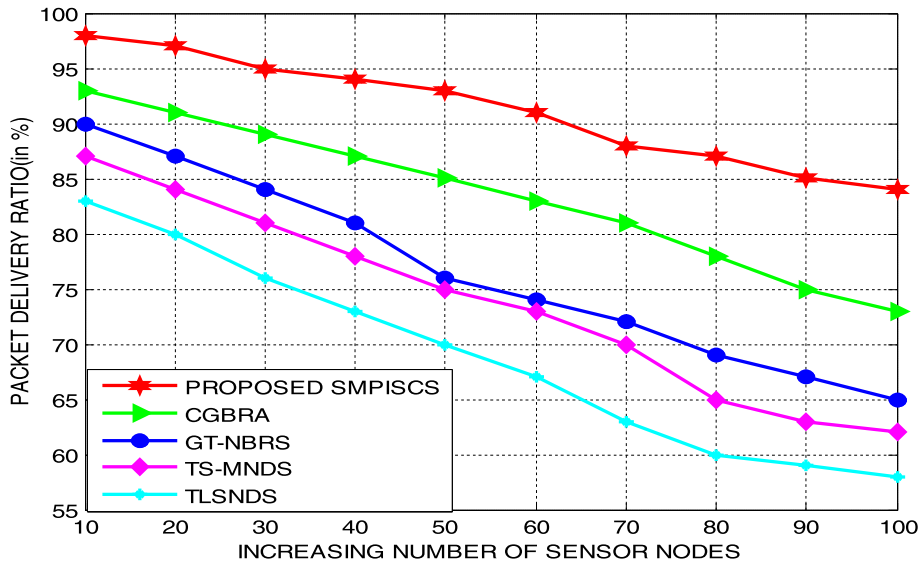

Fig. 3 SMPISCS-Packet delivery ratio (number of sensor nodes)

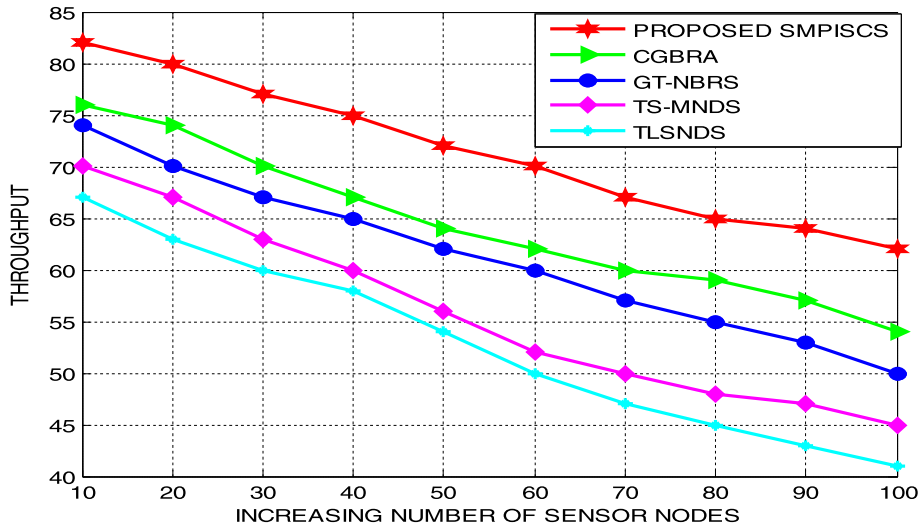

Fig. 4 SMPISCS-Throughput (number of sensor nodes)

SMPISCS in assuring significant packet delivery rate and throughput compared to CGBRA, GT-NBRS, TS-MNDS and TLSNDS scheme. This result proves that the packet delivery rate of SMPISCS is improved to about 11%, 13%, 16%, 18% compared to CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes. The throughput is also found to get enhanced by 9%, 11%, 14% and 17% compared to the benchmarked schemes due to the forecasting ability of SMPISCS which is ensured by the Semi-Markov modeling of the detection process are highlighted in Figs. 7 and 8.

The routing overhead and energy consumption rate of SMPISCS studied under the impact of different number of selfish sensor nodes of the network. The result infers the suitability of SMPISCS in minimizing routing overhead and energy utilization rate due to its dominance in reducing the number of re-transmissions. The result confirms that the routing overhead of SMPISCS is reduced to the significant level of 9%, 12%, 14% and 16% compared to CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes. The energy consumptions of SMPISCS also seem to get reduced by 10%, 13% and 17% higher than CGBRA, GT-NBRS, TS-MNDS and TLSNDS schemes are presented in Figs. 9 and 10.

Finally, the potential of SMPISCS investigated through co-operation degree under different detection levels of selfish behavior using network lifetime is represented using Figs. 11, 12 and 13.

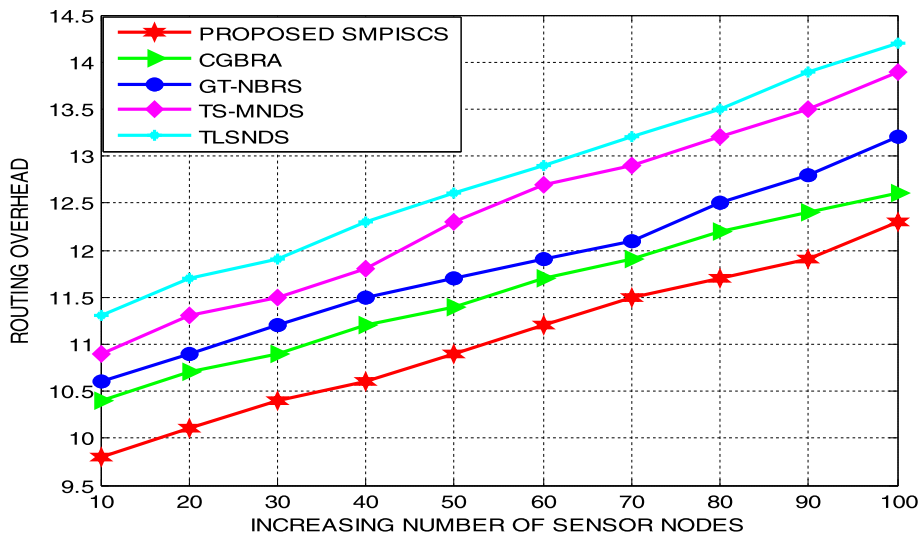

Fig. 5 SMPISCS-Routing Overhead (number of sensor nodes)

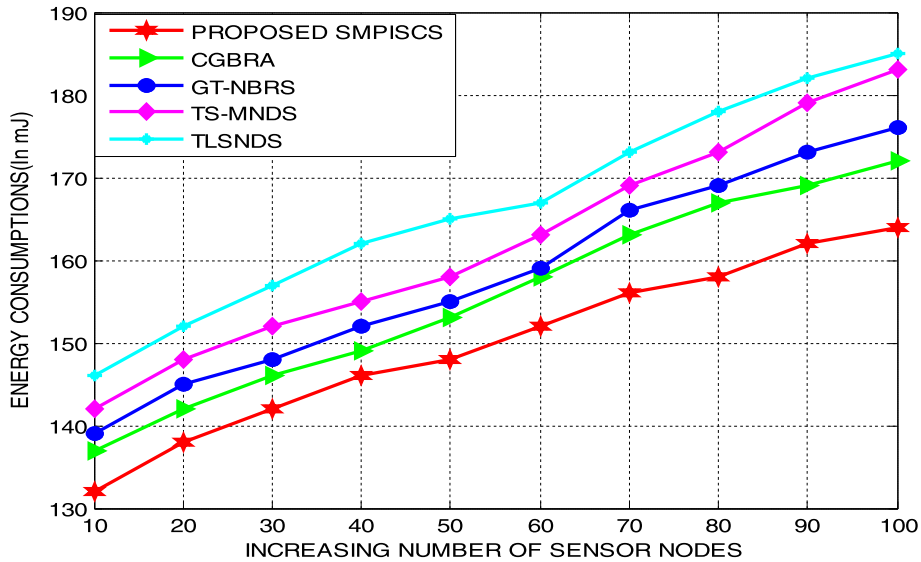

Fig. 6 SMPISCS-Energy consumptions (number of sensor nodes)

The results from Fig. 11 presents the network lifetime of SMPISCS under the cooperation degree in 0.3 and ensure that the rate of detection and isolation of selfish nodes enforced by SMPISCS is significant in enhancing the cooperation of degree to a mean level of 3.82%, 4.5%, 5.4% and 6.3% greater than CGBRA, GT-NBRS, TS-MNDS and TLSNDS. This enhancement in network lifetime under the impact of different detection thresholds are made feasible by SMPISCS mainly through the employment of uniformly distributed exponential parameter-based Semi-Markov Chain used for diagnosing selfish activity of selfish nodes. Fig. 12 highlights the improvement in network lifetime facilitated by SMPISCS under the co-operation degree of 0.6. The results portray that the incorporation of probe diagnostic time in SMPISCS improves the detection rate to a phenomenal level and enforces rapid detection and isolation of selfish nodes at an average of 4.2%, 5.8%, 6.4% and 6.8% greater than CGBRA, GT-NBRS, TS-MNDS and TLSNDS. This enhancement in network lifetime of SMPISCS is nearly

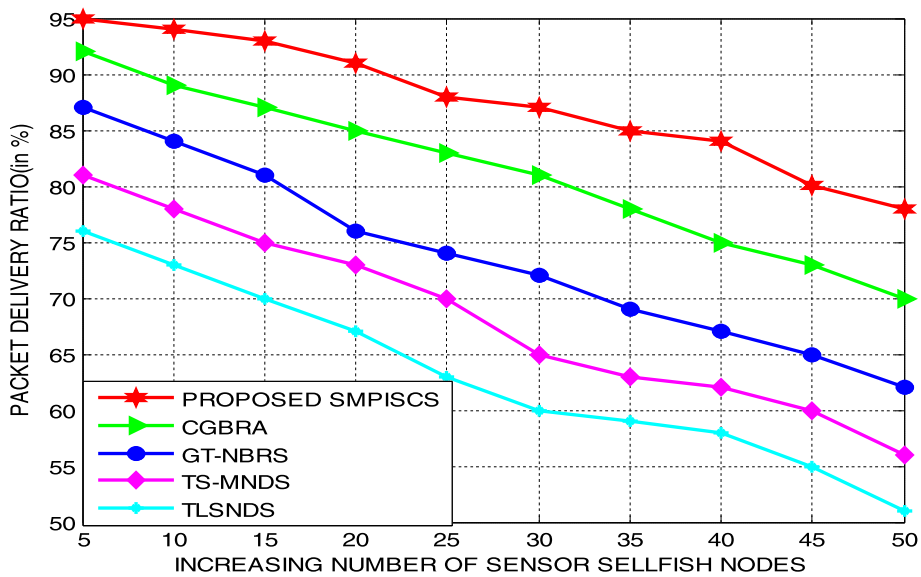

Fig. 7 SMPISCS-Packet Delivery Ratio (with selfish sensor nodes)

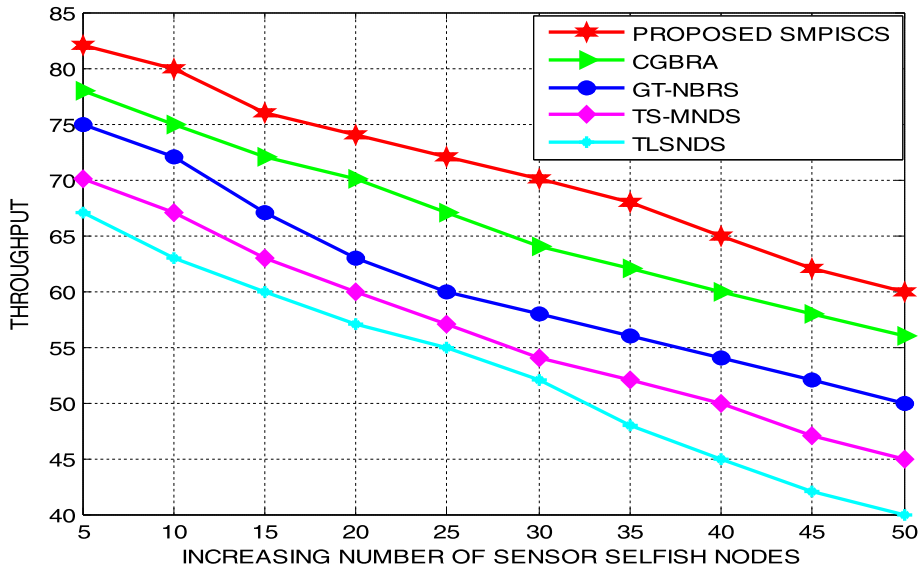

Fig. 8 SMPISCS-Throughput (with selfish sensor nodes)

5–7% more significant than its performance facilitated under the co-operation degree of 0.3. Likewise, Fig. 13 highlights the improvement in network lifetime facilitated by SMPISCS under the co-operation degree of 0.9. The results ensures a maximum level of detection and routing isolation of selfish nodes to an appreciable mean level of 4.6%, 5.4%, 6.2% and 7.3% greater than CGBRA, GT-NBRS,TS-MNDS and TLSNDS. This improvement in network lifetime enabled by SMPISCS is about 3–5% and 8%–11% higher than its performance in the co-operation degree of 0.6 and 0.3 respectively.

In addition, the detection rate of SMPISCS confirmed under different degrees of thresholds used for selfish behavior isolation. The results ensure that SMPISCS is capable of enhancing better detection rate of 8%, 13%, 16% and 19% compared to CGBRA,GT-NBRS, TS-MNDS and TLSNDS. This rapid rate of detection in SMPISCS is solely due to the convergence of probe-based diagnosis about selfish nodes from Semi-Markov Process to a Semi-Markov Chain. SMPISCS is also found to possess this maximum rate of detection due the level of

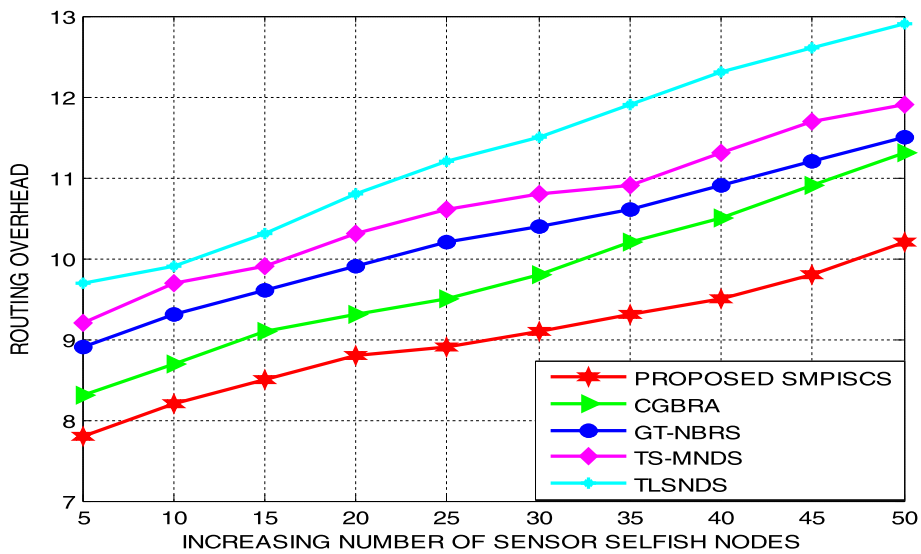

Fig. 9 SMPISCS-Routing Overhead (with selfish sensor nodes)

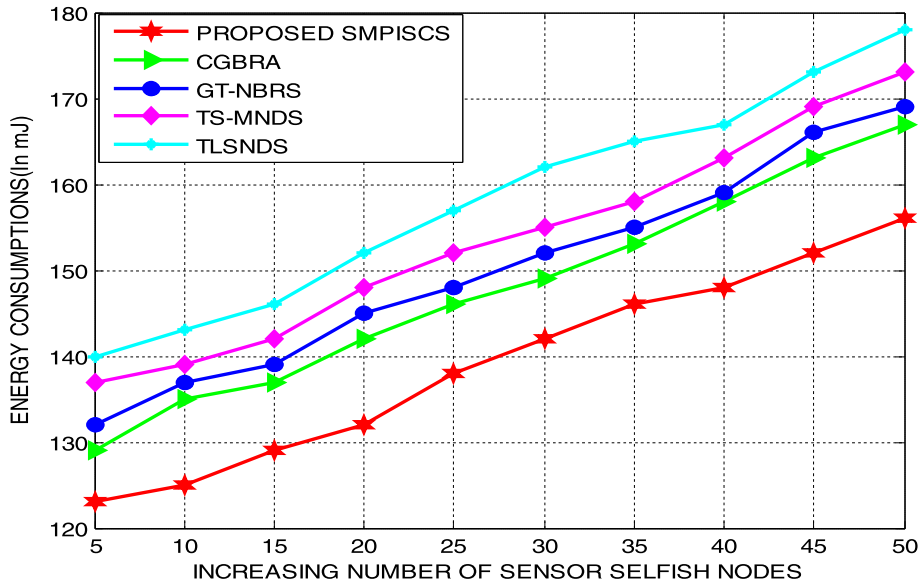

Fig. 10 SMPISCS-Energy Consumptions (with selfish sensor nodes)

co-operation enforced by the interacting nodes of the sensor network through the deployment of probe-routines are shown in Fig. 14.

The predominant performance of the proposed SMPISCS under an increasing number of sensor nodes and selfish sensor nodes is determined due to the following reasons as listed below.

i) The proposed SMPISCS scheme is capable of estimating the selfish intent of sensor nodes in an adaptive way at a dynamic time rate depending on the number of sensor nodes that get increased in the network.
ii) The proposed SMPISCS scheme is potential computation of transition probability depending on the number of selfish nodes in the sensor network.
iii) The increasing rate of packet delivery and throughput bears that the proposed SMPISCS model progresses the network lifetime compared to other specified models as in Figs. 11, 12 and 13.
iv) Selfish Sensor Node detection rate also has been addressed in experimentation by varying the

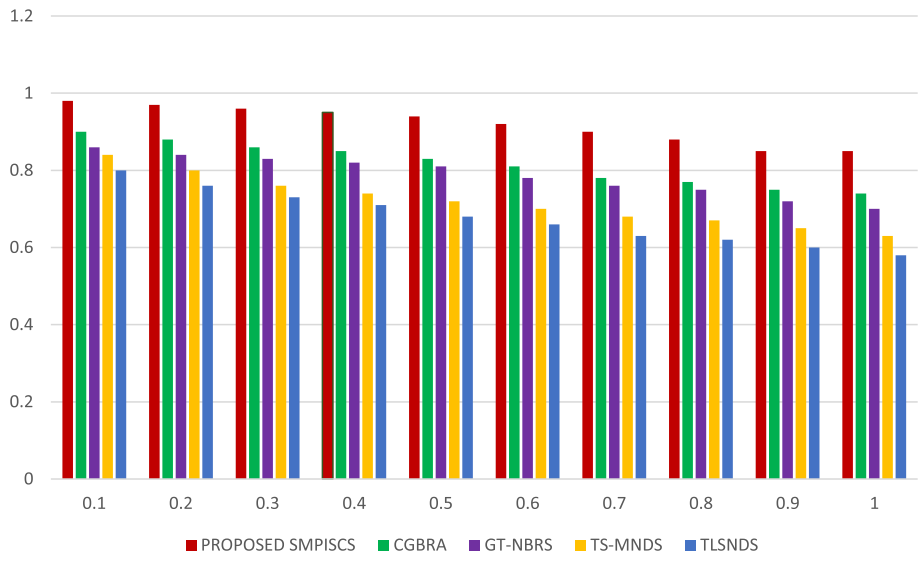

Fig. 11 SMPISCS-(Co-operation degree-0.3)-Network Lifetime

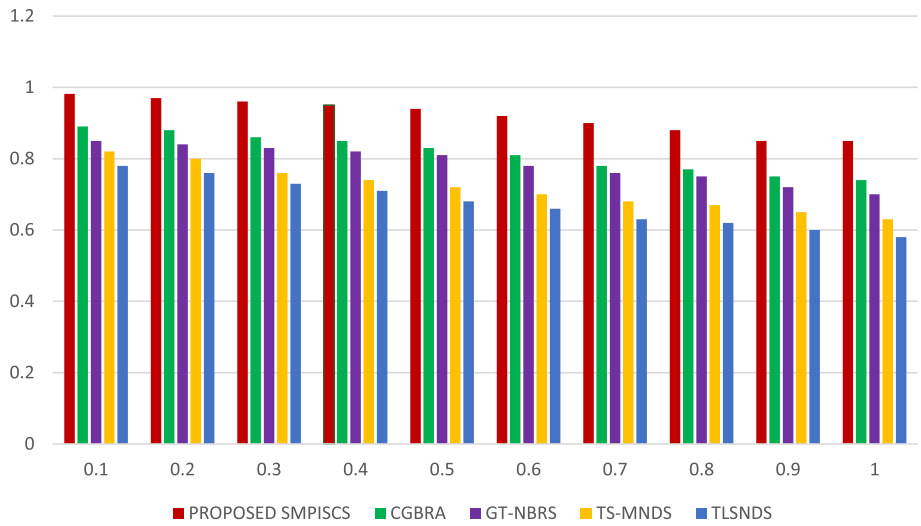

Fig. 12 SMPISCS-(Co-operation degree-0.6)-Network Lifetime

threshold. The proposed SMPISCS model bears a good improvisation comparatively with other models which uses exponential smoothing average method as in Fig. 14.

Conclusion

SMPISCS proposed in this paper is an attempt to prolong the network lifetime by effectively forecasting the selfish intent of sensor nodes and efficiently isolating them from the routing activity for enforcing co-operation. SMPISCS performs the act of predicting selfishness through the incorporation of probe routine which possess non-exponentially distributed diagnostic time interval and from the derivation of characteristic probabilities that are not influenced by the uniformly distributed diagnostic time. The evaluation results of SMPISCS estimated through varying degrees of co-operation level ensures its potential in prolonging the network lifetime at the mean rate of 10% higher than TFTBD, IBSBD and IBNBD. The results of SMPISCS confirm its maximum average detection rate of 26% which is comparably superior to most of the contributions of the literature proposed for detecting selfish intent of sensor nodes for the threshold 0.9. The performance evaluation of SMPISCS also unveils its capability in reducing the routing overhead and energy

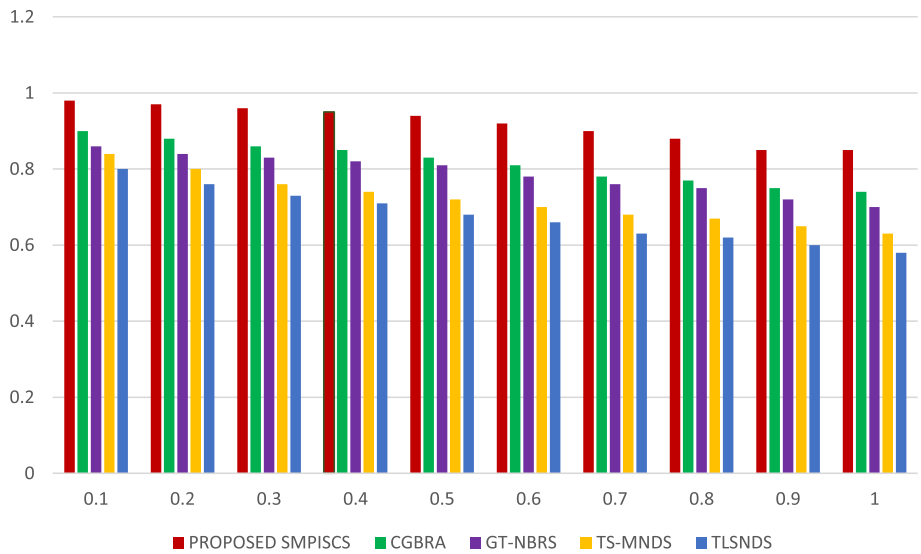

Fig. 13 SMPISCS-(Co-operation degree-0.9)-Network Lifetime

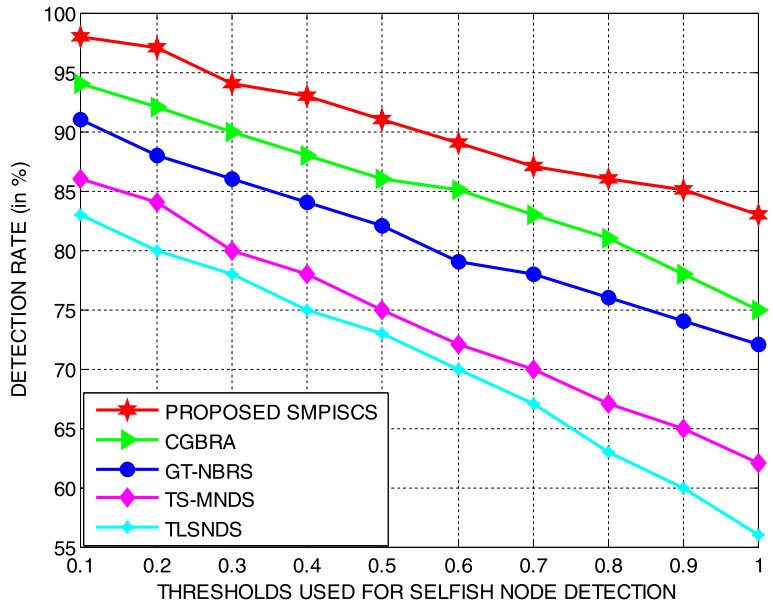

Fig. 14 SMPISCS-Detection Rate (Under different detection Thresholds)

consumptions by 16% and 13% compared to the schemes used for analysis. The process of predicting selfishness of sensor nodes is planned to be forecasted through grey theory in the near future and it is also planned to be focused on investigating the role and suitability of statistical reliability factors for enabling effective detection.

Acknowledgements
Not applicable.

Funding
Not applicable.

Availability of data and materials
Not applicable.

Authors' contributions
Both authors read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Received: 12 November 2018 Accepted: 15 January 2019
Published online: 28 January 2019

References

Arun Korath D, Vineeth KV (2011) A survey on detecting selfish nodes in wireless sensor networks using different trust methodologies. Ind J Appl Res *4*(1):193–194
Chen B, Mao J, Guo N, Qiao G, Dai N (2013a) An incentive detection mechanism for cooperation of nodes selfish behavior in wireless sensor networks. 2013 25th (CCDC) 1(2):23–32
Chen B, Mao J, Guo N, Qiao G, Dai N (2013b) An incentive detection mechanism for cooperation of nodes selfish behavior in wireless sensor networks. 2013 25th Chin Contr Decision Conf (CCDC) 1(2):23–32
Chen Z, He M, Liang W, Chen K (2015) Trust-aware and low energy consumption security topology protocol of wireless sensor network. J Sens 2015:1–10
Chen Z, Qiu Y, Liu J, Xu L (2011) Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game. Comput Mathematics Appl 62(9):3378–3388
Duan J, Yang D, Zhu H, Zhang S, Zhao J (2014a) TSRF: a trust-aware secure routing framework in wireless sensor networks. Int J Distrib Sens Netw 2014:1–14
Eswari T, Vanitha V (2013) A novel rule based intrusion detection framework for Wireless Sensor Networks. 2013 Int Conf Inform Commun Embedded Syst (ICICES) 1(1):1–13
George CM, Kumar M (2013) Cluster based Location privacy in Wireless Sensor Networks against a universal adversary. 2013 Int Conf Inform Commun Embedded Systems (ICICES) 2(1):45–54
Guo Y, Ma J, Wang C, Yang K (2013) Incentive-based optimal nodes selection mechanism for threshold key management in MANETs with selfish nodes. Int J Distrib Sens Netw *9*(5):34–46
Heinzelman W, Chandrakasan A, Balakrishnan H (2002) An application-specific protocol architecture for wireless microsensor networks. IEEE Trans Wirel Commun *1*(4):660–670
Ju L, Li H, Liu Y, Xue W, Li K, Chi Z (2010) An Improved Intrusion Detection Scheme Based on Weighted Trust Evaluation for Wireless Sensor Networks. 2010 Proc 5th Int Conf Ubiquitous Inform Technol and Appl 3(2):11–24
Li FP, Chang G, Yao L, Gao F (2012) Cooperative game-based routing approach for wireless sensor network. Int J Comput Appl Technol 44(2):101
Lin C, Wu G, Pirozmand P (2015) GTRF: a game theory approach for regulating node behavior in real-time wireless sensor networks. Sensors 15(6):12,932–12,958
Pal R (2009) Analyzing steady state probability distributions of context-sensitive probabilistic Boolean networks. Gen Sign Proc Stat, 2009. GENSIPS 2009. IEEE Int Workshop on IEEE 2009:1–4
Prathap U, Shenoy PD, Venugopal KR (2016) CMNTS: catching malicious nodes with trust support in wireless sensor networks. 2016 IEEE Region 10 Symp (TENSYMP) 2(1):12–24
Qiu Y, Chen Z, Xu L (2010) Active Defense Model of Wireless Sensor Networks Based on Evolutionary Game Theory. 2010 Int Conf Comput Intel Softw Eng 2(1):13–23
Reindl P, Nygard K, Du X (2010) Defending malicious collision attacks in wireless sensor networks. 2010 IEEE/IFIP Int Conf Embedded Ubiquitous Comput 3(1):13–24
Rikli N, Alnasser A (2016) Lightweight trust model for the detection of concealed malicious nodes in sparse wireless ad hoc networks. Int J Distrib Sens Netw 12(7):12,932–12,958

Tripathi M, Gaur MS, Laxmi V, Sharma P (2013) Detection and countermeasure of node misbehaviour in clustered wireless sensor network. ISRN Sensor Netw 2013:1–9
Wereley N, Walker B (1988) Approximate semi-Markov chain reliability models. Proc 27th IEEE Conf Decision Contr 2(1):23–45
Zhang J, Shankaran R, Orgun MA, Varadharajan V, Sattar A (2010) A dynamic trust establishment and management framework for wireless sensor networks. 2010 IEEE/IFIP Int Conf Embed Ubiquitous Comput 2(3):31–48
Zhang M, Zheng R, Li Y, Wu Q, Song L (2016) R-bUCRP: a novel reputation-based uneven clustering routing protocol for cognitive wireless sensor networks. J Sens 2016:1–9